UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/500,954	09/03/2004	Alexander Shipp	117-512	1417

23117 7590 10/30/2008

NIXON & VANDERHYE, PC
901 NORTH GLEBE ROAD, 11TH FLOOR
ARLINGTON, VA 22203

EXAMINER	
BROMELL, ALEXANDRIA Y	

ART UNIT	PAPER NUMBER
2167	

MAIL DATE	DELIVERY MODE
10/30/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/500,954	SHIPP, ALEXANDER	
	Examiner	Art Unit	
	ALEXANDRIA Y. BROMELL	2167	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *08 July 2008*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,2,5-8 and 11-16* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,2,5-8 and 11-16* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *7/08/04* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Response to Arguments

Applicant's arguments, see Remarks, filed July 8, 2008, with respect to the rejection(s) of claim(s) 1 - 2, 5 – 8, and 11 - 16 have been fully considered and are persuasive. Therefore, the rejection has been withdrawn. However, upon further consideration, a new ground(s) of rejection is made in view of Skoudis et al.

Claim Rejections - 35 USC § 101

35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

Claims 1 – 2 and 5 - 6 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter.

Claims 1 – 2 and 5 - 6 are rejected under 35 USC 101 for being "software per se".

The claimed invention as in claims 1 – 2, 5 - 6 is addressed to "an anti-malware file scanning computer system" that can be interpreted as referring to lines of programming within a computer system, rather than referring to the system as a physical object. The claimed invention is directed to, "a computer database " and "means for processing," and "means for signaling" therefore, the claims are deemed to read as pure software systems, with no clear limitations that read on some sort of hardware. The claims do not provide hardware such as a processor.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (a) the invention was known or used by others in this country, or patented or described in a printed publication in this or a foreign country, before the invention thereof by the applicant for a patent.

Claims 1 - 2, 5 – 8, and 11 - 16 are rejected under 35 U.S.C. 102(a) as being anticipated by Ed Skoudis et al. ("Malware: Fighting Malicious Code," Prentice Hall, 2003).

With respect to claim 1, Skoudis teaches a) a computer database containing records of known executable programs which are deemed to be not malware and criteria by which a file being processed can be determined to be an instance of one of those programs, the criteria including at least one characteristic signature associated with each said instance (i.e. document signatures are collected in a database for antivirus scanner, Chapter 2: Viruses: Defending against Viruses: Virus Signatures), b) means for processing a file being transferred between computers, the means b) comprising a file recogniser operative to determine whether the file being processed is an instance of a known program by checking the contents of the file being processed for the presence of said at least one characteristic signature associated with the said instances (i.e. document signature is compared with signatures in virus signature database to determine if it, or its file type is a potential malware specimen, Chapter 2: Viruses: Defending against Viruses: Virus Signatures), and a difference checker operative, in the case that the file recogniser determines the file being processed to be

an instance of a known program, to check whether the file is an unchanged version of that known program (i.e. file current state and baseline are compared to determine if file needs to be monitored, Chapter 2: Viruses: Defending against Viruses: Integrity Verification), and c) means for signalling the file, depending on the determination made by the processing means, as being likely to be not malware if it is an unchanged version of a known file, likely to be malware if it is a changed version of a known file, or of unknown status if it is not determined as being an instance of a known file (i.e. the computer computes fingerprints in the form of checksums or cryptographic hashes of files that need to be monitored if a file version has been changed, Chapter 2: Viruses: Defending against Viruses: Integrity Verification).

With respect to claim 2, Skoudis teaches d) means for processing a file being transferred between computers to determine whether it is considered to be, or considered possibly to be, malware, and wherein the means d) is operative to subject a file to processing if the file is signaled by the signalling means c) as being of unknown status (i.e. if the status of the file is unknown and needs to be monitored, fingerprints to that file are recorded in a baseline database, and alerts may be issued, Chapter 2: Viruses: Defending against Viruses: Integrity Verification).

With respect to claim 5, Skoudis teaches wherein the difference checker is operative to generate a checksum for the entire file under consideration or for at least one selected region thereof, and to compare the checksum or checksums with those of entries in the database (i.e. a checksum is computed for files that need to be monitored, which is recorded in a baseline database, after a comparison is performed to a

previously calculated value, an alert may be issued, Chapter 2: Viruses: Defending against Viruses: Integrity Verification).

With respect to claim 6, Skoudis teaches including an exception list handler operative to determine, in relation to a file which the processing means b) has determined is a changed version of a known file, whether that file has characteristics matching an entry in an exception list of files, the signalling means c) being operative to signal the file as malware only if it is not in the exception list or as being of unknown status otherwise (i.e. after a file version has been identified as changed, the antivirus software may be signaled to check the file more closely, to determine if it is the type with malicious code, Chapter 2: Viruses: Defending against Viruses: Integrity Verification, Virus Signatures).

With respect to claim 7, Skoudis teaches maintaining a computer database containing records of known executable programs which are deemed to be uninfected and criteria by which a file being processed can be determined to be an instance of one of those programs, the criteria including at least one characteristic signature associated with each said instance (i.e. document signatures are collected in a database for antivirus scanner, Chapter 2: Viruses: Defending against Viruses: Virus Signatures), processing a file being transferred between computers by determining whether the file being processed is an instance of a known program by checking the contents of the file being processed for the presence of said at least one characteristic signature associated with the said instances (i.e. document signature is compared with signatures in virus signature database to determine if it, or its file type is a potential malware

specimen, Chapter 2: Viruses: Defending against Viruses: Virus Signatures), and checking, in the case that the file is determined to be an instance of a known program, whether the file is an unchanged version of that known program (i.e. file current state and baseline are compared to determine if file needs to be monitored, Chapter 2: Viruses: Defending against Viruses: Integrity Verification), signalling the file, depending on the determination made by the processing means, as being likely to be not malware if it is an unchanged version of a known file; likely to be malware if it is a changed version of a known file, or of unknown status if it is not determined as being an instance of a known file, and storing the determination that the file is likely to be not malware, is likely to be malware or is of unknown status (i.e. the computer computes fingerprints in the form of checksums or cryptographic hashes of files that need to be monitored if a file version has been changed, Chapter 2: Viruses: Defending against Viruses: Integrity Verification).

With respect to claim 8, Skoudis teaches processing a file being transferred between computers to determine whether it is considered to be, or considered possibly to be, malware, if the file is signalled by the signalling step c) as being of unknown status (i.e. if the status of the file is unknown and needs to be monitored, fingerprints to that file are recorded in a baseline database, and alerts may be issued, Chapter 2: Viruses: Defending against Viruses: Integrity Verification).

With respect to claim 11, Skoudis teaches the step of checking whether the file being processed is an instance of a known program comprises generating a checksum for the entire file under consideration or for at least one selected region thereof, and

comparing the checksum or checksums with those of entries in the database (i.e. a checksum is computed for files that need to be monitored, which is recorded in a baseline database, after a comparison is performed to a previously calculated value, an alert may be issued, Chapter 2: Viruses: Defending against Viruses: Integrity Verification).

With respect to claim 12, Skoudis teaches using an exception list to determine, in relation to a file which the processing step b) has determined is a changed version of a known file, whether that file has characteristics matching an entry in an exception list of files, and wherein, in the signalling step c), the file is signalled as malware if it is not in the exception list or as being of unknown status otherwise (i.e. after a file version has been identified as changed, the antivirus software may be signaled to check the file more closely, to determine if it is the type with malicious code, Chapter 2: Viruses: Defending against Viruses: Integrity Verification, Virus Signatures).

With respect to claim 13, Skoudis teaches a computer database containing records of known executable programs which are deemed to be not malware and criteria by which a file being processed can be determined to be an instance of one of those programs, the criteria including at least one characteristic signature associated with each said instance (i.e. document signatures are collected in a database for antivirus scanner, Chapter 2: Viruses: Defending against Viruses: Virus Signatures), a processor for processing a file being transferred between computers, the processor being operative to determine whether the file being processed is an instance of a known program by checking the contents of the file being processed for the presence of said at

least one characteristic signature associated with the said instances and, in the case that the file being processed is determined to be an instance of a known program, to check whether the file is an unchanged version of that known program (i.e. document signature is compared with signatures in virus signature database to determine if it, or its file type is a potential malware specimen, Chapter 2: Viruses: Defending against Viruses: Virus Signatures), said processor, depending on the determination, identifying the file being processed as (i) likely to be not malware if it is an unchanged version of a known file, (ii) likely to be malware if it is a changed version of a known file, or (iii) of unknown status if it is not determined as being an instance of a known file (i.e. file current state and baseline are compared to determine if file needs to be monitored, the computer computes fingerprints in the form of checksums or cryptographic hashes of files that need to be monitored if a file version has been changed, Chapter 2: Viruses: Defending against Viruses: Integrity Verification).

With respect to claim 14, Skoudis teaches a file-scanning subsystem for scanning files identified by the processor as being of unknown status to determine whether the scanned files are malware (i.e. files are scanned to determine if files have malware, Chapter 2: Viruses: Defending against Viruses: Integrity Verification, Virus Signatures).

With respect to claim 15, Skoudis teaches records for files which are instances of programs determined by the file-scanning system not to be malware are added to the computer database (i.e. computer database stores file types which indicate malware

specimens and ordinary files, Chapter 2: Viruses: Defending against Viruses: Virus Signatures).

With respect to claim 16, Skoudis teaches the processor assigns a score to a file identified as likely to be malware (i.e. checksum scores may be used to flag potential malware, Chapter 2: Viruses: Defending against Viruses: Integrity Verification).

Conclusion/Contact Information

Any inquiry concerning this communication or earlier communications from the examiner should be directed to ALEXANDRIA Y. BROMELL whose telephone number is (571)270-3034. The examiner can normally be reached on M-F 8-4.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, John R. Cottingham can be reached on 571-272-7079. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Alexandria Y Bromell/
Examiner, Art Unit 2167
October 24, 2008
/John R. Cottingham/
Supervisory Patent Examiner, Art Unit 2167

/S. A. A./
Primary Examiner, Art Unit 2162